DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy #3: Servers (Except Web Servers)

1. References:

   a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

   b. AR 25-2, Information Assurance, 14 November 2003.

   c. AR 380-67, Personnel Security Program, 9 September 1988.

   d. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

   e. DOD Instruction 8500.2, “Information Assurance (IA) Implementation”, 6 February 2003.

   f. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

   g. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

   h. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

   i. 4ID Policy # 5: Passwords.

2. Purpose of Policy:

   Servers are primary devices used by 4ID to establish data communications connectivity between individual office automation users and shared applications and devices (like printer servers and file servers). Server configurations impact the ease-of-use, risk management, operating effectiveness, and reliability of network resources provided by 4ID. This policy guides the deployment, documentation, operation, and maintenance of 4ID servers other than web servers.

3. Applicability:

   a. This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

   b. This policy does not apply to web server operations. Web servers have unique vulnerabilities and are addressed in a separate policy memorandum.

4. Responsibilities:

   a. 4ID is responsible for implementing and operating office automation servers and configurations as required to support 4ID organization data networking and data connectivity requirements.

   b. Information Assurance Manager (IAM) will:

(1) Ensures the server policy is written that describes the intended functionality of the server and that the server as installed enforces that policy.

(2) Ensures that the server system administrator (SA) receives training to operate the server.

c. Information Assurance Security Officer (IASO) will:

(1) Ensure that the servers are operated and maintained according to the vendor's specifications and organizational requirements.

(2) Ensure the certification and accreditation is completed and current on the server installation.

(3) Working with the server system administrator, ensure that the server audit log is reviewed frequently.

(4) Report any security incidents involving the server as required by the organizational security regulations, and to the IAM.

(5) Ensure the server security policy is implemented and carried out properly. Continuously evaluate the server security environment. Make recommendations to the IAM as appropriate.

d. Server System Administrator will:

(1) Understand and monitor the configuration of the server.

(2) Each workstation shall be configured with user ID and password access controls that are compliant with the 4ID password policy.

(3) Ensure that the server is continuously afforded effective physical security.

(4) Ensure that configuration management processes are used and server configuration documentation is up-to-date.

(5) Make frequent backups of data and files on the server and ensure that server software integrity is maintained.

(6) Respond to any alarms or alerts from the server software as quickly as possible.

(7) In coordination with the IASO, ensure adequate security is maintained over the server.

(8) Install IAVA patches and corrective patches and upgrades to the server software as required.

(9) Review the audit logs on the server on a daily basis.

(10)Report any attacks or incidents on the server to the server IASO.

(11)Ensure anti-virus software is installed and operational. Anti-virus software and signatures will be kept current from a trusted source, such as the ACERT web site.

5. Policy:

a. Security Policy Required: There must be an explicit and well-defined security policy enforced for each operating platform.

(1) All guest accounts shall be disabled.

(2) Administrator accounts shall be renamed if the system makes provision for it.

(3) Accounts shall be locked after 5 unsuccessful attempts within a 30-minute period and the System Administrator and IASO notified.

(4) Only system administrators shall unlock accounts.

(5) Audit records shall be generated to document when account lockouts occur.

(6) Remote administration of servers over the NIPRNet, Internet, etc., shall be accomplished via a secure communications path (e.g., VPN, etc.).

b. Accountability: Audit information shall be retained and protected so that actions affecting security can be traced to the responsible party. Each network server shall be scanned at least twice a year using approved security scanning software. The purpose of server audits is to confirm the degree to which actual configurations are reflected in baseline configuration files. Further, they verify the degree to which changes in server configuration have been documented and approved in the configuration management processes.

c. Baseline:

(1) All servers shall be loaded and configured with a standard baseline image that is consistent with the most recently ACERT approved security patches and fixes. The current Army security baseline configurations for server operating systems are developed and maintained by Regional Computer Emergency Response Team – Europe (RCERT-E) and can be found at https://www.rcert-e.army.mil.

(2) Microsoft product baselines can be found at https://iassure.usareur.army.mil/security/microsoft/.

(3) Only servers with built-in auditing and logging capability shall be deployed.

(4) Servers shall be configured to utilize built-in auditing capabilities in accordance with the current governing policy on operational controls.

(5) Servers shall have the capability to allow discretionary access control to the directory and file level.

(6) Systems Administrators shall include updated Emergency Repair Disks (ERDs) for all Microsoft OS-based servers to assist in recoverability during system failures.

d. Documentation: A baseline of all server documentation shall be maintained by the SA. This documentation shall include, but is not limited to, Standard Operating Procedures (SOPs), Server System Administration Guides, Server Deployment Guides, and Server Change Management documents. Documentation shall reflect updates as server configurations and baseline changes are implemented.

e. Continuous Protection:

(1) The "trusted" mechanisms that enforce these basic requirements shall be continuously protected against tampering and/or unauthorized changes. Attempts to modify the system services, whether successful or not, shall be recorded in security logs. This provides a documented record of all user and system changes attempted and made.

(2) Security, application, and system audit logs shall be copied nightly. Systems shall be backed up on a regular basis and backups stored in a secure off-site location.

f. Physical Security Policy: Servers shall be located in secured facilities with controlled access.

g. Documentation and Configuration Management:

(1) Maintenance of up-to-date configuration documentation and configuration management records is the responsibility of the SA.

(2) Server configuration documentation shall be retained by the SA and audited annually by the IAM or designee to ensure that proper configuration management controls are being used.

(3) The SA or IASO shall review server level security logs on a daily basis at a minimum. The SA or IASO shall take immediate action to resolve security events detected through the review of security logs. Once the log is reviewed and unexplained security events resolved, it shall be validated for retention or destruction in accordance with log retention policies.

(4) Changes to the configuration baseline shall be in accordance with the 4ID Configuration Management Plan (CMP) and coordinated and/or approved by the 4ID Configuration Control Board (CCB).

6. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding